

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-332747

(43)Date of publication of application : 30. 11. 2000

(51)Int. CI. H04L 9/32

H04L 9/08

H04L 12/46

H04L 12/28

H04L 12/56

(21)Application number : 11-142486

(71)Applicant : MITSUBISHI ELECTRIC CORP  
NIPPON TELEGR & TELEPH  
CORP <NTT>

(22)Date of filing : 21. 05. 1999

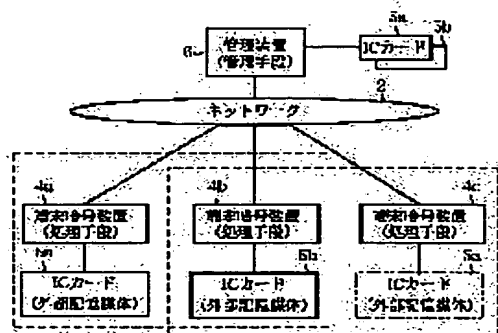
(72)Inventor : BOKU BIJIYOU  
WATANABE AKIRA  
MIYAGAWA AKIKO  
ATOZAWA SHINOBU  
SAIJO TOMOYUKI  
OKA KATSUYA  
SEGUCHI ARIYOSHI

## (54) CLOSED-AREA COMMUNICATION SYSTEM

## (57)Abstract:

PROBLEM TO BE SOLVED: To allow different terminals to conduct the same closed area communication, even when a work site is changed by introducing external storage media to the title system so as to authenticate a user belonging to a prescribed group in the closed area communication.

SOLUTION: This closed-area communication system is configured with IC cards 5a, 5b that store information for user authentication which is an object of the closed area communication, a plurality of terminal encryption units 4a-4c, that encrypt communication data and decode the encrypted data according to contents of an operating table 13 produced on the basis of the information stored in the IC cards 5a, 5b, and a management unit 6 that is connected to the



terminal encipherment units 4a-4c via a network 2 and issues the IC cards 5a, 5b to a user which is an object of the closed-area communication.

---

#### LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's  
decision of rejection]

[Kind of final disposal of application  
other than the examiner's decision of  
rejection or application converted  
registration]

[Date of final disposal for  
application]

[Patent number]

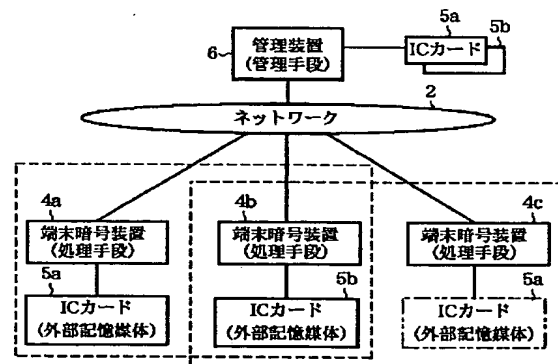
[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against  
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office



## 【特許請求の範囲】

【請求項1】 所定のグループに属するユーザ間で閉域通信を行う際の、閉域通信の対象となるユーザ認証のための情報を保持する外部記憶媒体と、ネットワークに接続され、前記外部記憶媒体に保持された前記ユーザ認証のための情報をもとに生成した動作テーブルの内容に従って通信データの暗号および復号の処理を行う複数の処理手段と、前記外部記憶媒体を発行する、前記処理手段に前記ネットワークを介して接続される管理手段とを備えた閉域通信システム。

【請求項2】 外部記憶媒体に、閉域通信の対象となるユーザ認証のための情報として、ユーザID、認証秘密情報、管理手段情報を保持させ、管理手段は、前記外部記憶媒体が処理手段に挿入されると、当該外部記憶媒体の保持する情報をもとに、閉域通信に必要な動作テーブルを前記処理手段に配送するものであることを特徴とする請求項1記載の閉域通信システム。

【請求項3】 管理手段は、ユーザのグループIDおよびそれに対応する暗号鍵を処理手段に配送するものであり、前記処理手段は、それらの情報を通信相手の処理手段または中継装置との間で交換し、前記通信相手の処理手段との間の閉域通信に必要な動作テーブルを自動生成するものであることを特徴とする請求項2記載の閉域通信システム。

【請求項4】 処理手段は、外部記憶媒体が抜き取られたことを検出すると、現在保持している動作テーブルを消去するものであることを特徴とする請求項2記載の閉域通信システム。

【請求項5】 管理手段は、外部記憶媒体を発行する際に、当該外部記憶媒体の内容をパスワードで暗号化するとともに、前記パスワードの初期パスワードの決定を行うものであり、処理手段は、前記パスワードを変更するパスワード変更手段を有するものであることを特徴とする請求項2記載の閉域通信システム。

【請求項6】 外部記憶媒体としてICカードを用いたことを特徴とする請求項1から請求項5のうちのいずれか1項記載の閉域通信システム。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、機密保護を目的とするネットワークシステムにおいて、所定のグループに属するユーザに対して閉域通信を提供する閉域通信システムに関するものである。

【0002】

【従来の技術】図11は、例えば特開平11-055322の明細書および図面に示された、従来の閉域通信シ

ステムを示すシステム構成図である。図において、1a、1b、1cは閉域通信を行う端末であり、2はこれらの端末1a～1cが収容されるネットワークである。3a、3b、3cは端末1a～1cとネットワーク2の間の中継経路上に配置された暗号装置であり、暗号装置3aはグループIDが1の暗号鍵、暗号装置3bはグループIDが1および2の暗号鍵、暗号装置3cはグループIDが2の暗号鍵をそれぞれ保有している。なお、上記端末1a～1cおよび暗号装置3a～3cはその各々を区別しない場合には、それぞれ端末1あるいは暗号装置3と表記する。

【0003】図12は上記暗号装置3の内部構成を示すブロック図である。図において、10は暗号/復号処理部、11は透過中継処理部、12は廃棄処理部である。13は通信データの処理方法を示す動作テーブル、14は自動学習処理部である。なお、初期の時点の動作テーブル13には、通信データの処理方法はなにも登録されていないものとする。15はネットワーク2側のインタフェースであるパブリックポート、16は端末1側のインタフェースであるローカルポート、17、18は送受信処理部である。

【0004】次に動作について説明する。従来の閉域通信システムでは、ネットワーク2に収容されている通信端末1a～1c間の中継経路上に配置された暗号装置3a～3cが保持するグループID情報を収集し、収集したグループID情報に対応した暗号鍵のID情報に基づいて動作テーブル13を自動学習し、その学習結果に基づいて自動生成した動作テーブル13を用いて通信するものである。ここで、各暗号装置3a～3cに割り当てられるグループIDおよび暗号鍵の実体はあらかじめ配送されており、各暗号装置3a～3cはそれらの情報を一組または複数組、動作テーブル13に保持している。

【0005】端末1aと端末1bの間で閉域通信を行う場合、端末1aから端末1bへの通信データは暗号装置3aにおいて、その動作テーブル13の内容に従って、暗号/復号処理部10でIDが1の暗号鍵を用いて暗号化され、暗号化通信データとして端末1b宛てに送信される。暗号装置3bでは暗号/復号処理部10において、この暗号装置3aからの暗号化通信データをその動作テーブル13の内容に従って、元の通信データに復号し、それを端末1bへ送信する。同様に、端末1bから端末1aへの通信データは、暗号装置3bでその動作テーブル13の内容に従って、IDが1の暗号鍵により暗号化されて暗号装置3aへ送られ、その動作テーブル13の内容に従って、IDが1の暗号鍵により復号され、端末1aに達する。

【0006】なお、このような従来の閉域通信システムに関係のある技術が記載されている文献としては、この他にも、例えば特開平9-247141号公報、特開平10-171717号公報などがある。

【0007】

【発明が解決しようとする課題】従来の閉域通信システムは以上のように構成されているので、端末1a~1c間の暗号通信を中継する暗号装置3a~3cにあらかじめ登録されているグループID、またはあらかじめ配送されているグループIDによる暗号鍵によって閉域通信を実現しているため、ユーザが使用する端末1a~1cが固定されてしまうという課題があった。

【0008】この発明は、上記のような課題を解決するためになされたもので、外部記憶媒体を導入して、所定のグループに属するユーザに対して閉域通信におけるユーザ認証を行うことにより、作業場所が変わっても、異なる端末より同一の閉域通信が行える閉域通信システムを得ることを目的とする。

【0009】

【課題を解決するための手段】この発明に係る閉域通信システムは、ユーザ認証のための情報を保持する外部記憶媒体をユーザに持たせ、当該情報をもとに生成した動作テーブルの内容に従って、通信データの暗号および復号の処理を行うことによって、異なる作業場所からでも同一の閉域通信ができるようにしたものである。

【0010】この発明に係る閉域通信システムは、ユーザID、認証秘密情報、管理手段情報を保持した外部記憶媒体を処理手段に挿入したとき、管理手段より処理手段に対して、外部記憶媒体が保持する情報をもとに、閉域通信に必要な動作テーブルを配送するようにしたものである。

【0011】この発明に係る閉域通信システムは、管理手段から処理手段に対して、ユーザのグループIDおよびそれに対応する暗号鍵を配送し、処理手段はそれらの情報を通信相手の処理手段または中継装置との間で交換して、動作テーブルの自動生成を行うようにしたものである。

【0012】この発明に係る閉域通信システムは、外部記憶媒体の抜き取りを検出した処理手段が、保持している動作テーブルを消去するようにしたものである。

【0013】この発明に係る閉域通信システムは、管理手段に、外部記憶媒体を発行する際に外部記憶媒体の内容をパスワードで暗号化する機能、および初期パスワードを決定する機能を持たせ、処理手段に、パスワードの変更を行う機能を持たせたものである。

【0014】この発明に係る閉域通信システムは、ICカードを外部記憶媒体として用いるようにしたものである。

【0015】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態1. 図1は、この発明の実施の形態1による閉域通信システムの構成を示すシステム構成図である。

図において、2は閉域通信を行う所定のグループのメン

バであるユーザに対して、閉域通信を許容するネットワークであり、4a、4b、4cはそれぞれこのネットワーク2に收容されて、ユーザが閉域通信を行う端末の機能と、閉域通信に先立って暗号鍵情報を自動学習し、通信データの暗号/復号処理を行う暗号装置の機能とを併せ持った、処理手段としての端末暗号装置である。5a、5bは閉域通信を行うユーザが所有し、それを所有しているユーザにのみ閉域通信を可能とするための情報が格納された、外部記憶媒体としてのICカードであり、6は閉域通信を行うグループの登録を行い、当該グループのメンバーである各ユーザにこのICカード5a、5bを発行する管理手段としての管理装置である。なお、上記端末暗号装置4a~4cおよびICカード5a、5bはその各々を区別しない場合には、それぞれ端末暗号装置4あるいはICカード5と表記する。

【0016】図2は上記端末暗号装置4の内部構成を示すブロック図である。図において、10は通信データの暗号および復号処理を行う暗号/復号処理部である。11は通信データをそのまま透過的に中継する透過中継処理部であり、12は通信データを廃棄する廃棄処理部である。13は通信データの処理方法を示す動作テーブルであり、通信データの宛先となる端末暗号装置4と送信元となる端末暗号装置4のペア毎に、当該通信データの処理方法が登録されるものである。なお、初期の時点では、この動作テーブル13には送信データの処理方法は何も登録されていないものとする。14はこの動作テーブル13の自動学習処理部であり、動作テーブル13に処理方法が登録されていない場合に起動されるものである。15はネットワーク2側のインタフェースであるバブリックポートであり、17、18は通信データの受信処理および送信処理を実施する送受信処理部である。なお、これら各部は、図12に同一符号を付して示した従来のそれらに相当する部分である。

【0017】また、19は閉域通信を行うユーザによってICカード5が挿入され、当該ICカード5に保持されている閉域通信を可能とするための情報の読み取りが行われるICカードリーダである。20はユーザによるこのICカードリーダ19へのICカード5の挿入を常に監視しながら、ICカード5より読み出された情報を処理するICカード処理部であり、このICカード処理部20はICカード5の内容を暗号化するためのパスワードを変更するパスワード変更手段としても機能する。21は従来のローカルポートの部分に配置されたPCI/Fであり、この端末暗号装置4とユーザとのマン・マシンのインタフェースをとるものである。なお、ICカード処理部20はこのPCI/F21と送受信処理部18の接続点に、ICカードリーダ19が読み出した情報を処理して出力している。

【0018】図3は管理装置6によってユーザに発行されるICカード5に書き込まれる情報を示す説明図であ

り、図において、30は管理装置6でユーザ登録を行った際に登録されたユーザのユーザID、31はユーザ認証のために用いる認証秘密情報、32は管理装置6のIPアドレスを示す、管理手段情報としての管理装置IPアドレスである。

【0019】図4は管理装置6の有する機能を示す説明図である。図において、40はユーザに発行するICカード5に必要な情報の書き込みを行う、ICカード書き込み処理機能である。41は閉域通信に参加を希望するユーザの新規登録を行ない、各ユーザの閉域通信グループの登録を行うとともに、閉域通信グループ構成情報の表示、および変更を行う構成情報保存編集機能である。42は端末暗号装置4に対して、閉域通信グループのグループID、および閉域通信用の暗号鍵を配送する暗号鍵配送機能である。

【0020】次に動作について説明する。管理装置6は、あらかじめ次の処理を行っておくものとする。すなわち、まず最初に、その構成情報保存編集機能41によって、当該閉域通信システムを利用することを希望する新規ユーザの登録を行う。登録が終わったユーザに対しては、そのICカード書き込み処理機能40を用いて、図3に示したユーザID30、認証秘密情報31、および管理装置IPアドレス32を、管理装置6において管理者によって決められたパスワード（初期パスワード）を用いて暗号化してICカード5に書き込み、そのICカード5を該当するユーザに発行する。ICカード5を発行した後、各ユーザごとにそれが所属するグループのグループIDを定義しておく。

【0021】この実施の形態1では、第1のユーザにはICカード5aを、第2のユーザにICカード5bをそれぞれ発行し、これら第1のユーザと第2のユーザを同一の閉域通信グループに登録するものとする。

【0022】次に、端末暗号装置4に対して閉域通信用のグループIDおよび暗号鍵を配送する動作について説明する。ここで、図5は端末暗号装置4へのグループIDおよび暗号鍵の配送動作を示すシーケンス図であり、この場合、ICカード5aの持ち主である第1のユーザ側の動作について示している。

【0023】第1のユーザが管理装置6より発行してもらった、当該第1のユーザ用のICカード5aを端末暗号装置4aのICカードリーダ19に差し込むと、当該端末暗号装置4aのICカード処理部20は、その差し込まれたICカード5aの情報をICカードリーダ19を介して読み込み、ユーザ認証のためのパスワードの入力を促すパスワード要求100を、PC1/F21を介して第1のユーザに送る。第1のユーザはこのパスワード要求100に従って自身のパスワード101を入力する。入力されたパスワード101はPC1/F21を介してICカード処理部20に送られ、ICカード処理部20は第1のユーザよりパスワード101が返送されて

くると、それを用いてICカードリーダ19で読み出したICカード5aの内容の解読を行う。

【0024】端末暗号装置4aのICカード処理部20は、このICカード5aから読み込んだ第1のユーザのユーザID30をパラメータ配送要求102とし、それを管理装置IPアドレス32に基づいて管理装置6のIPアドレス宛てに配送する。管理装置6は構成情報保存編集機能41を用いて、この端末暗号装置4aから受け取ったユーザID30による検索を行って、第1のユーザが所属しているグループのグループIDとそれに対応する暗号鍵を決定する。管理装置6はさらに、それらグループIDと暗号鍵の情報を、そのユーザID30に対応する認証秘密情報31を用いて暗号化し、それをパラメータ配送暗号化103として端末暗号装置4aに送る。

【0025】このパラメータ配送暗号化103を受けた端末暗号装置4aは、ICカード5aが保持している認証秘密情報31を用いて受信したデータを復号し、グループIDおよび暗号鍵を得る。そして、管理装置6に対して確認応答104を返送するとともに、取得したグループIDおよび暗号鍵を用いて、自動学習処理部14による動作テーブル13の自動学習を行い、生成された動作テーブル13による閉域通信を開始する。

【0026】次に、上記動作テーブル13による閉域通信の動作について説明する。ここで、図6は第1のユーザと第2のユーザとの間における閉域通信の動作を示すシーケンス図である。まず、この図6に示すように、第1のユーザより端末暗号装置4aに対して、第2のユーザ宛ての通信データ110が入力される。なお、この通信データ110は、図2では図示を省略した通信データバッファ内に一旦保持される。通信データ110を受信した端末暗号装置4aは内部の動作テーブル13の検索を行う。初期の時点ではこの動作テーブル13には、端末暗号装置4aと端末暗号装置4bの間の通信処理方法は登録されていないので、端末暗号装置4aは、図7に示す鍵探索パケット111を作成して端末暗号装置4bに送信する。

【0027】図7は上記鍵探索パケット111のフォーマットを示すデータ構成図であり、鍵探索パケット111は、図示のように、種別201、宛先202、送信元203より成るヘッダ200と、送信元アドレス211、宛先アドレス212、送信元端末暗号装置暗号鍵情報213、宛先端末暗号装置暗号鍵情報214より成るデータ部210によって形成されている。なお、この図7に示す例では、ヘッダ200の種別201には探索パケットが、宛先202には端末暗号装置4bが、送信元203には端末暗号装置4aが設定され、データ部210の送信元アドレス211には端末暗号装置4aのアドレスが、宛先アドレス212には端末暗号装置4bのアドレスが、送信元端末暗号装置暗号鍵情報213には端

末暗号装置4aの持つ暗号鍵のIDである1が設定されている。また、この端末暗号装置4bに送信される鍵探索バケット111では、端末暗号装置4aと端末暗号装置4bの間の通信処理方法が登録されていないので、宛先端末暗号装置暗号鍵情報214には何も設定されていない。

【0028】端末暗号装置4bではこの鍵探索バケット111を受信すると、図8に示すように、そのデータ部210の宛先端末暗号装置暗号鍵情報214に自身の暗号鍵のIDである1と2を設定する。端末暗号装置4bはこの宛先端末暗号装置暗号鍵情報214の設定が行われ、当該鍵探索バケット111のデータ部210をコピーして鍵探索応答バケット112を作成する。

【0029】図9はこの鍵探索応答バケット112のフォーマットを示すデータ構成図であり、図7、図8に示した鍵探索バケット111と同様のヘッダ200とデータ部210によって形成されている。ただし、ヘッダ200の種別201には探索応答バケットが、宛先202には端末暗号装置4aが、送信元203には端末暗号装置4bが設定され、データ部210では端末暗号装置4bのアドレスが送信元アドレス211となり、端末暗号装置4aのアドレスが宛先アドレス212となっている。

【0030】端末暗号装置4bは、生成した鍵探索応答バケット112の送信元端末暗号装置暗号鍵情報213に、自身の暗号鍵のIDである1または2と同じ暗号鍵のIDが設定されていないかどうかを検索する。この場合、端末暗号装置4aが鍵探索バケット111に設定した、当該端末暗号装置4aの暗号鍵のIDである1がコピーされて、鍵探索応答バケット112の送信元端末暗号装置暗号鍵情報213に設定されている。このように、端末暗号装置4bの暗号鍵のIDである1が、鍵探索応答バケット112の送信元端末暗号装置暗号鍵情報213に設定されているので、端末暗号装置4bは自身の動作テーブル13に、端末暗号装置4aと端末暗号装置4bの間の通信データをIDが1の暗号鍵で暗号/復号することを登録するとともに、その鍵探索応答バケット112をヘッダ200の宛先202に従って、端末暗号装置4aに送信する。

【0031】端末暗号装置4aは、この鍵探索応答バケット112を受信すると、その宛先端末暗号装置暗号鍵情報214に自身の暗号鍵のIDである1と同じ暗号鍵のIDが設定されているかどうかを検索する。この場合、当該宛先端末暗号装置暗号鍵情報214には端末暗号装置4bが設定した暗号鍵のIDである1と2の2つが設定されている。従って、端末暗号装置4aは自身の動作テーブル13に、端末暗号装置4aと端末暗号装置4bの間の通信データをIDが1の暗号鍵で暗号/復号することを登録する。

【0032】端末暗号装置4aは通信データバッファ内

に保持しておいた第1のユーザからの通信データ110を、暗号/復号処理部10において、動作テーブル13の内容に従って、IDが1の暗号鍵を用いて暗号化して暗号通信データ113を生成し、それを端末暗号装置4b宛てに送信する。また、受信した鍵探索応答バケット112のヘッダ200では、その宛先202が当該端末暗号装置4aになっているので、端末暗号装置4aはこの鍵探索応答バケット112をその廃棄処理部12において廃棄する。

【0033】一方、端末暗号装置4aで暗号化された暗号通信データ113を受け取った端末暗号装置4bは、自身の動作テーブル13の内容に従って暗号/復号処理部10において、IDが1の暗号鍵を用いてその暗号通信データ113を通信データ110に復号し、PC1/F21より第2のユーザに提示する。

【0034】同様に、第2のユーザから第1のユーザへの通信データ114は、端末暗号装置4bでその動作テーブル13の内容に従って、IDが1の暗号鍵によって暗号化され、暗号通信データ115として端末暗号装置4aに送られる。端末暗号装置4aではその暗号通信データ115を、自身の動作テーブル13の内容に従ってIDが1の暗号鍵により復号し、復号した通信データ114を第1のユーザに提示する。

【0035】次に、このようにして第2のユーザと閉域通信を行っている第1のユーザが、その作業場所を変えた場合の動作について説明する。第1のユーザは作業場所を変える場合、元の作業場所に備えられた端末暗号装置4aのICカードリーダー19から、自身に発行されたICカード5aを抜き取り、それを移動先の作業場所に備えられた端末暗号装置4cのICカードリーダー19に挿入する。端末暗号装置4cはICカード5aが挿入されると、そのユーザID30より当該第1のユーザが所属しているグループIDを管理装置6より送ってもらう。これによって閉域通信の対象となるユーザ認証を行い、第1のユーザが同一の閉域通信グループのユーザであると認識されると、端末暗号装置4bのICカードリーダー19にICカード5bを挿入した第2のユーザとの閉域通信が可能になる。

【0036】以上のように、この実施の形態1によれば、ユーザにユーザID30、認証秘密情報31、管理装置IPアドレス32を保持したICカード5を発行して、ICカード5aの持ち主である第1のユーザと、ICカード5bの持ち主である第2のユーザを同一の閉域通信グループに登録し、第1のユーザがICカード5aを端末暗号装置4aに挿入すると、管理装置6から第1のユーザが所属しているグループIDを配送しているので、同一の閉域通信グループに属する第2のユーザとの閉域通信が可能になり、また、第1のユーザがその作業場所を変えた場合でも、移動先の作業場所に設置された端末暗号装置4cにICカード5aを挿入すると、管理

装置 6 からその端末暗号装置 4 c に対して第 1 のユーザが所属しているグループ ID が配送されるため、ユーザの使用する端末（端末暗号装置）が固定されることがなくなり、端末に依存することなく第 2 のユーザとの間で同一の閉域通信が可能になるなどの効果が得られる。

【0037】実施の形態 2. 次に、この発明の実施の形態 2 による閉域通信システムについて説明する。この実施の形態 2 は、閉域通信終了時の処理に関するものであり、図 10 はそのようなこの実施の形態 2 における、端末暗号装置 4 の IC カードリーダ 19 から IC カード 5

を抜き取った場合の動作を示すシーケンス図である。  
【0038】まず、この図 10 に示すように、当該閉域通信を終了したい第 1 のユーザが端末暗号装置 4 a の IC カードリーダ 19 より IC カード 5 a を抜き取る。端末暗号装置 4 a ではこの IC カード 5 a の抜き取りを、その IC カード処理部 20 で検出すると、管理装置 6 に対して ENDTRAP 120 を送信する。この ENDTRAP 120 を受信した管理装置 6 は ENDTRAP 応答 121 を生成し、それを端末暗号装置 4 a に返送する。管理装置 6 からこの ENDTRAP 応答 121 を受け取った端末暗号装置 4 a は、内蔵する動作テーブル 13 を消去するとともに、当該閉域通信を終了する。このようにして閉域通信を終了した端末暗号装置 4 a は、その透過中継処理部 11 を用いて、閉域通信グループに属さない一般の端末と同様の動作を行う。

【0039】このように、この実施の形態 2 によれば、端末暗号装置 4 はその IC カードリーダ 19 より IC カード 5 a を抜き取るだけで動作テーブル 13 が消去されるため、簡単に閉域通信を終了して、一般の端末と同様の動作を行うことが可能となる効果が得られる。

【0040】実施の形態 3. 次に、この発明の実施の形態 3 について説明する。この実施の形態 3 はユーザ側からの、管理装置 6 で決定したパスワードの変更処理に関するものである。このパスワードの変更はユーザによって、PC I/F 21 を介して会話形式で行われ、その制御はパスワード変更手段として機能する IC カード処理部 20 によって処理される。すなわち、端末暗号装置 4 の IC カードリーダ 19 に IC カード 5 が挿入されると、IC カード処理部 20 より PC I/F 21 を介して、パスワードの入力がユーザに対して要求される。ユーザによってパスワードが入力されると、IC カード処理部 20 は PC I/F 21 を介して、パスワードの変更に関するメニューを表示する。このメニューを参照したユーザが変更ありを選択すると、IC カード処理部 20 は PC I/F 21 を介して、新たなパスワードの入力を要求する。ユーザによって新たなパスワードが入力されると、IC カード処理部 20 はそれに基づくパスワードの変更処理を行う。

【0041】以上のように、この実施の形態 3 によれば、管理装置 6 で決定したパスワードを、ユーザ側で必

要に応じて、会話形式による簡単な操作で変更することが可能になり、セキュリティの向上が図れるという効果が得られる。

【0042】実施の形態 4. なお、上記各実施の形態では、端末暗号装置 4 は管理装置 6 からグループ ID および暗号鍵の配送を受け、配送された情報をもとに動作テーブル 13 を自動学習する場合について説明したが、管理装置 6 が各端末暗号装置 4 の動作テーブル 13 を何らかの手段であらかじめ保持していれば、パラメータ配送で上記動作テーブル 13 を直接各端末暗号装置 4 に配送するようにしてもよく、上記各実施の形態と同様の結果を得ることができる。

【0043】また、上記各実施の形態では、端末の機能と暗号装置の機能を併せ持った端末暗号装置 4 を用いて閉域通信システムを構成したものについて説明したが、従来の場合と同様に、端末暗号装置 4 に代えて端末と暗号装置を個別に設けるようにしてもよく、上記各実施の形態と同様の結果を奏する。

【0044】さらに、上記各実施の形態では、管理装置 6 から端末暗号装置 4 に配送したユーザのグループ ID およびそれに対応する暗号鍵の情報を、通信相手の端末暗号装置 4 との間で直接交換して、動作テーブル 13 の自動生成するものについて説明したが、中継装置を介して交換するようにしてもよく、上記各実施の形態と同様の結果を奏する。

【0045】

【発明の効果】以上のように、この発明によれば、ユーザ認証のための情報を保持する外部記憶媒体をユーザに持たせ、当該情報をもとに生成した動作テーブルの内容に従って、通信データの暗号および復号の処理を行うように構成したので、ユーザは使用する端末（処理手段）が固定されることがなくなり、任意の端末を用いて閉域通信を行うことが可能な閉域通信システムが得られる効果がある。

【0046】この発明によれば、外部記憶媒体にユーザ ID、認証秘密情報、管理手段情報を保持させ、当該外部記憶媒体を挿入した時、それが保持する情報をもとに、管理手段より処理手段に動作テーブルを配送させるように構成したので、外部記憶媒体が保持する情報をもとに配送された動作テーブルに従って閉域通信を行うことが可能となり、作業場所が変わっても異なる端末（処理手段）によって同一の閉域通信を行うことができるという効果がある。

【0047】この発明によれば、ユーザのグループ ID とそれに対応する暗号鍵を管理手段から処理手段に配送して、それらの情報を通信相手の処理手段または中継装置との間で交換することで、動作テーブルの自動生成を行うように構成したので、上記グループ ID を用いた自動学習により生成された動作テーブルに従って閉域通信を行うことが可能となり、作業場所が変わっても異なる



端末（処理手段）によって同一の閉域通信を行うことができるという効果がある。

【0048】この発明によれば、外部記憶媒体が抜き取られると、保持している動作テーブルの消去を行うように構成したので、外部記憶媒体を挿入した時には閉域通信を行い、外部記憶媒体を抜き取った時には一般の通信を行うことが可能になるという効果がある。

【0049】この発明によれば、管理手段において決定した、外部記憶媒体の内容を暗号化するためのパスワードを、処理手段にて変更可能に構成したので、ユーザ側でこのパスワードを必要に応じて変更することにより、セキュリティを向上させることができるという効果がある。

【0050】この発明によれば、外部記憶媒体としてICカードを用いるように構成したので、外部記憶媒体の取り扱いが容易となり、その管理もしやすいものになるなどの効果がある。

#### 【図面の簡単な説明】

【図1】 この発明の実施の形態1による閉域通信システムの構成を示すシステム構成図である。

【図2】 実施の形態1における端末暗号装置の内部構成を示すブロック図である。

【図3】 実施の形態1における管理装置よりユーザに発行されるICカードに書き込まれる情報を示す説明図である。

【図4】 実施の形態1における管理装置の有する機能を示す説明図である。

\*【図5】 実施の形態1における端末暗号装置へのグループIDおよび暗号鍵の配送動作を示すシーケンス図である。

【図6】 実施の形態1におけるユーザ間の閉域通信の動作を示すシーケンス図である。

【図7】 実施の形態1における宛先端末暗号装置暗号鍵情報が未設定の鍵探索バケットのフォーマットを示すデータ構成図である。

10 【図8】 実施の形態1における宛先端末暗号装置暗号鍵情報が設定済みの鍵探索バケットのフォーマットを示すデータ構成図である。

【図9】 実施の形態1における鍵探索応答バケットのフォーマットを示すデータ構成図である。

【図10】 この発明の実施の形態2におけるICカードを抜き取った場合の動作を示すシーケンス図である。

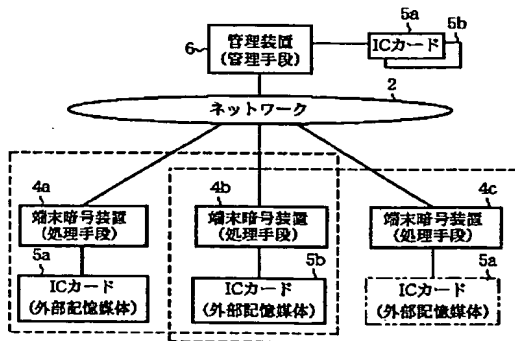
【図11】 従来の閉域通信システムの構成を示すシステム構成図である。

【図12】 従来の閉域通信システムにおける暗号装置の内部構成を示すブロック図である。

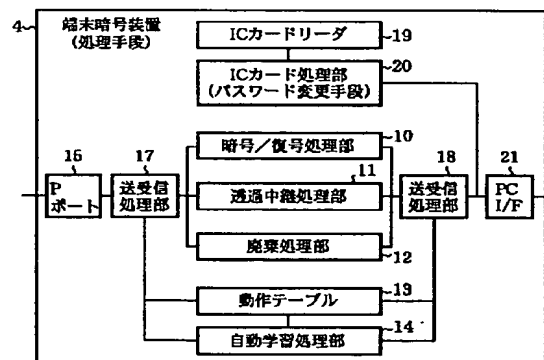
20 【符号の説明】

2 ネットワーク、4、4a、4b、4c 端末暗号装置（処理手段）、5、5a、5b ICカード（外部記憶媒体）、6 管理装置（管理手段）、13 動作テーブル、20 ICカード処理部（パスワード変更手段）、30 ユーザID、31 認証秘密情報、32 管理装置IPアドレス（管理手段情報）、110、114 通信データ。

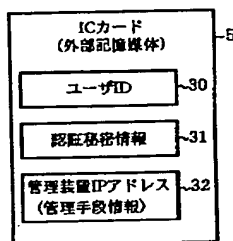
【図1】



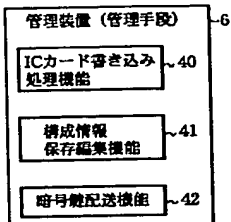
【図2】



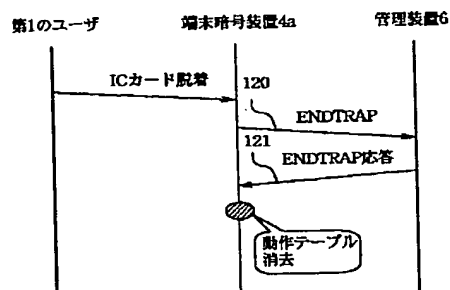
【図3】



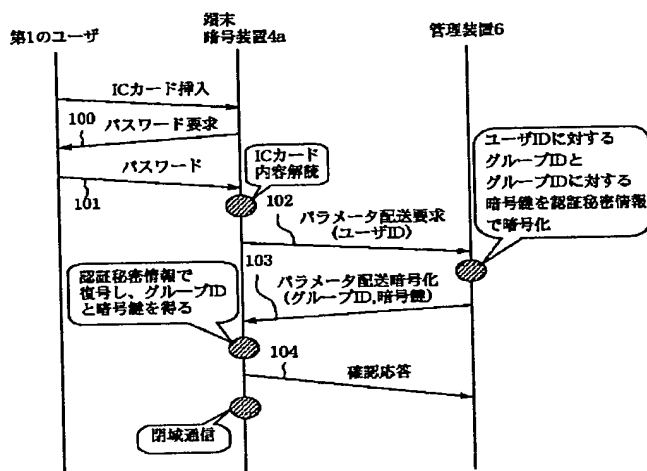
【図4】



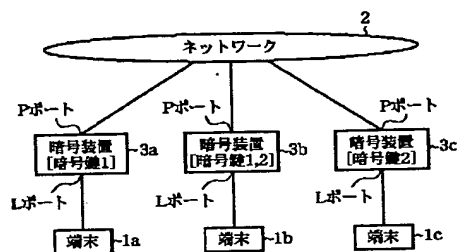
【図10】



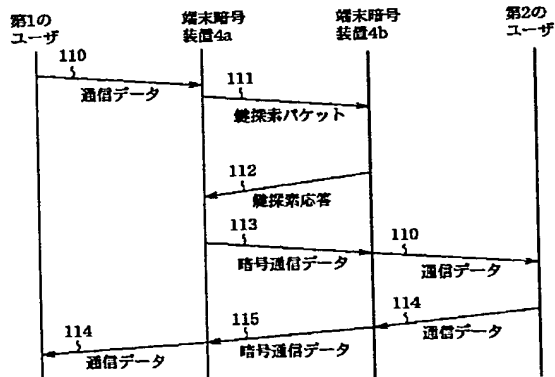
【図5】



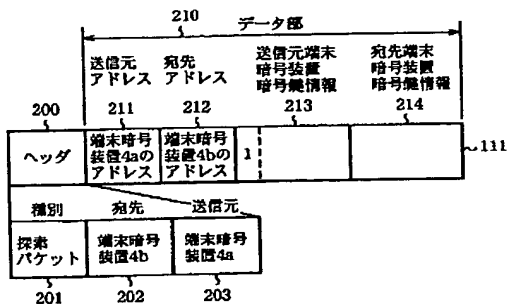
【図11】



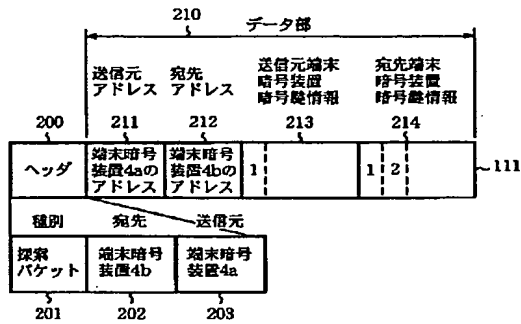
【図6】



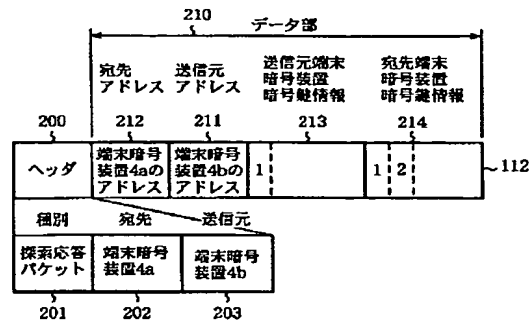
【図7】



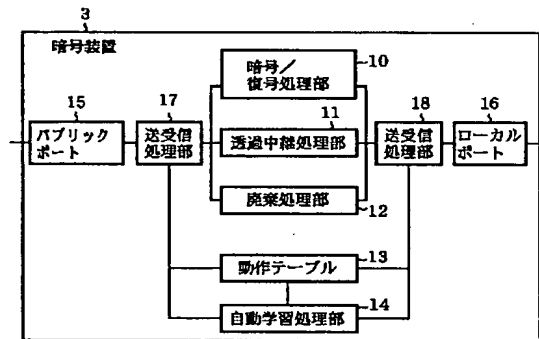
【図8】



【図9】



【図12】



フロントページの続き

- (72)発明者 渡邊 晃  
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
- (72)発明者 宮川 明子  
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
- (72)発明者 後沢 忍  
東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内
- (72)発明者 西條 智幸  
東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

- (72)発明者 岡 克也  
東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内
- (72)発明者 瀬口 有美  
東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内
- Fターム(参考) 5J104 AA07 AA16 EA01 EA06 EA17  
EA22 KA01 MA02 MA06 NA03  
NA05 NA20 NA35 PA00  
5K030 GA15 GA16 HC01 HC13 KA01  
5K033 AA08 DA01 DB10 DB20

**This Page Blank (uspto)**